Error Avoiding Quantum Codes and Dynamical Stabilization of Grover's Algorithm

Michael Mussinger, Aldo Delgado and Gernot Alber
Abteilung für Quantenphysik, Universität Ulm, D-89069 Ulm, Germany

An error avoiding quantum code is presented which is capable of stabilizing Grover's quantum search algorithm against a particular class of coherent errors. This error avoiding code consists of states only which are factorizable in the computational basis. Furthermore, its redundancy is smaller than the one which is achievable with a general error correcting quantum code saturating the quantum Hamming bound. The fact that this code consists of factorizable states only may offer advantages for the implementation of quantum gates in the error free subspace.

I. INTRODUCTION

According to a suggestion of Feynman [1] quantum systems are not only of interest for their own sake but they might also serve for practical purposes. Thus they may be used for simulating other quantum systems which are less convenient to handle or they may be used for solving computational problems more efficiently than by any other classical means. Two well known examples demonstrating this latter point are Shor's factorization algorithm [2] and Grover's search algorithm [3].

Quantum systems which are capable of performing quantum algorithms are called quantum computers. So far several physical systems have been considered as potential candidates for quantum computers, such as trapped ions [4], nuclear spins of molecules [5] or in the context of cavity quantum electrodynamics atoms interacting with a single mode of the radiation field [6]. To describe the operation of a quantum computer theoretically it is advantageous to refrain from a detailed physical description of the particular quantum system involved. Thus, analogous to the spirit of computer science it is more useful to concentrate on those particular aspects which are essential for the performance of quantum computation. On this abstract level a generic quantum computer consists of m distinguishable smaller quantum systems which are frequently chosen as two-level systems with basis states $|1\rangle$ and $|0\rangle$, for example. The quantum information which can be stored in one of these two level systems is called a qubit. Thus the state space of a generic quantum computer is spanned by the so called computational basis which consists of the corresponding 2^m product states $|b_0\rangle = |0\ldots00\rangle$, $|b_1\rangle = |0\ldots01\rangle$, ... $|b_{2^m}\rangle = |1\ldots11\rangle$.

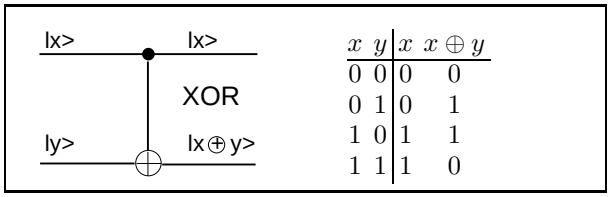
A typical quantum computation proceeds in several steps. Firstly, the quantum computer is prepared in an initial state. Secondly, a certain sequence of unitary transformations is performed which are called quantum gates and which usually entangle the m qubits. Thirdly, the final result is measured. Typically the solution of a particular computational problem is obtained with a certain probability only. A general quantum algorithm takes advantage of an essential feature of quantum theory, namely the interference between probability amplitudes and the fact that the dimensionality D of the state space of m distinguishable qubits increases exponentially with the number of qubits, i.e. $D = 2^m$. One of the best known quantum algorithms are the already mentioned Shor algorithm [2] and Grover's search algorithm [3,7]. In this latter algorithm a particular sequence of quantum gates enables one to find a specific item out of an unsorted database much faster than with any other known classical mean. This quantum algorithm was already realized experimentally for a small number of qubits [8].

One of the main practical problems one has to overcome in the implementation of quantum algorithms are non-ideal performances of the quantum gates [9] involved or random environmental influences which both tend to affect the relevant quantum coherence. To protect quantum computation against such errors two major strategies have been proposed recently, namely quantum error correction [10–12] and error avoiding quantum codes [13,14]. Quantum error correction rests on the assumption that nothing is known about the physical origin of the errors affecting the quantum computation. Its methods may be considered as an extension of classical error correction techniques to the quantum domain [11,12]. The approach of the error avoiding quantum codes is different. They rest on the assumption that the physical origin of the errors which affect the quantum computation is known. The main idea of this latter approach is to encode the logical information in one of those subspaces of the relevant Hilbert space which is not affected by the physical interactions responsible for the occurance of errors [13,14]. Both theoretical approaches to error correction rest on the concept of redundancy which is also fundamental for classical error correcting codes [15]. Provided the physical origin of the errors affecting a quantum computation is known it is expected that error avoiding codes offer more effective means for stabilizing quantum algorithms. This expectation is based on two facts. Firstly, there is no need for control measurements which are an essential ingredient for any error correcting code. Secondly, usually a smaller number of *physical* qubits is needed for the representation of a given number of *logical* qubits.

In the subsequent discussion it is demonstrated that this is indeed the case. By considering Grover's quantum search algorithm it is shown that non-ideal perturbations may be corrected dynamically in an efficient way

with the help of an appropriate error avoiding quantum code. As a particular example, we discuss coherent errors which may arise from systematic detunings of the physical qubits of the quantum computer from the frequency of the light pulses which realize the required quantum gates. It is shown that the corresponding error avoiding quantum code with the lowest degree of redundancy is more efficient in encoding quantum information than the corresponding optimal error correcting code which saturates the quantum Hamming bound. The proposed error avoiding quantum code consists of states only which are factorizable in the computational basis. In this respect it differs significantly from the recently proposed error avoiding code of Ref. [13], for example, which also involves entangled states. Such factorizable codes may offer practical advantages as far as the implementation of quantum gates in error avoiding subspaces is concerned.

The article is organized as follows: In Sec. II basic facts about Grover's quantum search algorithm are summarized. It is demonstrated that for large databases the dynamics of this quantum algorithm can be described by a two-level Hamiltonian which implies Rabi oscillations between the initial state and the search state. In Sec. III general ideas underlying the construction of error avoiding quantum codes are discussed. An efficient error avoiding quantum code is presented which is capable of stabilizing Grover's algorithm against a particular class of coherent errors. The redundancy of this code is discussed and compared with the one resulting from error correcting codes which saturate the quantum Hamming bound. Numerical examples demonstrating the stabilizing capabilities of this error avoiding quantum code are presented in Sec. IV.



x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

FIG. 1. Quantum mechanical version of the classical-XOR gate as an example for a quantum gate (CNOT gate): The input state $|x, y\rangle$ is mapped onto the output state $|x, x \oplus y\rangle$.

II. GROVER'S QUANTUM SEARCH ALGORITHM

Consider an unsorted database with N items and a certain item x_0 you are searching for. As a particular example you can imagine a telephone directory with N entries and a particular telephone number x_0 you are looking for. Furthermore, assume that you are given a black box, i.e. a so called oracle, which can decide whether an item is x_0 or not. Thus, in mathematical terms you are given a Boolean function

$$f(x) = \delta_{x,x_0} = \begin{cases} 1 & x = x_0 \\ 0 & x \neq x_0 \end{cases} \tag{1}$$

with $\delta_{a,b}$ denoting the Kronecker delta function. Usually the elements x of the database are assumed to be described by the N integers between zero and $N-1$. Assuming that each application of the oracle requires one elementary step a classical random search process will require $N-1$ steps in the worst case and one step in the best possible case. Thus, on the average a classical algorithm will need $N/2$ steps to find the searched item x_0. It has been shown by Grover [3] that with the help of his quantum search algorithm this task can be performed in $O(\sqrt{N})$ steps with a probability arbitrarily close to unity. The basic idea of this quantum algorithm is to rotate the initial state of the quantum computation in the direction of the searched state $|x_0\rangle$ by a sequence of unitary quantum versions of the oracle. It will become apparent from the subsequent discussion that apart from Hadamard transformations the dynamics of this rotation are analogous to a Rabi oscillation between the initially prepared state and the searched state $|x_0\rangle$. It has been shown by Zalka [16] that Grover's quantum search algorithm is optimal.

A. Characteristic gate sequence of Grover's search algorithm

In Grover's quantum search algorithm every element of the database is represented by a state of the computational basis of the quantum computer. Thus a database which is represented by m qubits has $N = 2^m$ distinguishable elements. The state $|0..0110..0\rangle$ of the computational basis, for example, corresponds to the element 0..0110..0 of the database in binary notation. The quantum oracle $\mathcal{U}_f$ is determined completely by the Boolean function of Eq.(1) and is represented by a quantum gate, i.e. by the unitary and hermitian transformation

$$\mathcal{U}_f : |x, a\rangle \rightarrow |x, f(x) \oplus a\rangle. \tag{2}$$

Thereby $|x\rangle$ is an arbitrary element of the computational basis and $|a\rangle$ is the state of an additional ancilla qubit which is discarded later. The symbol $\oplus$ denotes addition modulo 2. This unitary form of the oracle depends on the Boolean function $f(x)$. As far as complexity estimates are concerned it is assumed that this unitary transformation requires one elementary step. This assumption is analogous to the complexity estimate of the corresponding classical version of this search problem.

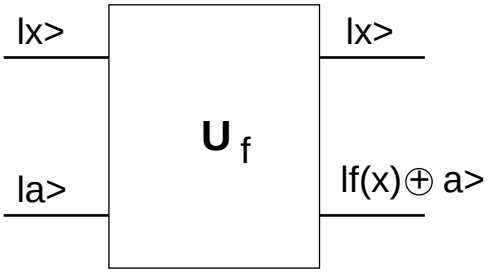


FIG. 2. Schematic representation of the quantum oracle $\mathcal{U}_f$: For $f(x) \equiv x$ this quantum gate reduces to the CNOT gate of Fig.1; for $|a\rangle \equiv |a_0\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$ it results in the conditional phase inversion I_{x_0} of Eq.(9) needed in Grover's algorithm.

For the subsequent discussion it is important to note that the elementary rotations in the direction of the searched quantum state $|x_0\rangle$ which are the key ingredient in Grover's algorithm can be performed with the help of this unitary oracle. Thus such a rotation can be performed without explicit knowledge of the state $|x_0\rangle$. Its implicit knowledge through the values of the Boolean function $f(x)$ is already sufficient. For large values of N it turns out that the number of elementary rotations needed to prepare state $|x_0\rangle$ is $O(\sqrt{N})$. To implement such an elementary rotation from the initial state $|s\rangle = |0...0\rangle$, for example, towards the final state $|x_0\rangle$ two different types of quantum gates are needed, namely *Hadamard* gates and *controlled phase inversions*.

A *Hadamard* gate is a unitary one-qubit operation. It produces an equal weighted superposition of the two basis states according to the rule

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3}$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4}$$

or in matrix notation

$$H^{(2)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

A m-qubit Hadamard gate $H^{(2^m)}$ is defined by the m-fold tensor product, i.e. $H^{(2^m)} = H^{(2)} \otimes ... \otimes H^{(2)}$. Thus, for two qubits, for example, $H^{(2^2)}$ is represented by the matrix

$$H^{(2^2)} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{5}$$

The Hadamard transformation is hermitian and unitary. An arbitrary matrix element $H_{i,j}^{(2^m)}$ of a Hadamard transformation may be written in the general form

$$H_{i,j}^{(2^m)} = \frac{1}{\sqrt{2^m}}(-1)^{i \odot j}. \tag{6}$$

Thereby i and j denote binary numbers and the multiplication $\odot$ is bitwise modulo 2, i.e. for $i = 1$, $j = 3$ and $m = 2$, one obtains $H_{1,3}^{(4)} = (1/2)(-1)^{(01 \odot 11)} = (1/2)(-1)^{(0 \cdot 1 + 1 \cdot 1)} = -1/2$. It has been shown by Grover [3] that this Hadamard transformation can be replaced by any other unitary one-qubit operation.

The remaining quantum gates needed for the implementation of the necessary rotation are *controlled phase inversions* with respect to the initial and searched states $|s\rangle = |0...0\rangle$ and $|x_0\rangle$. A controlled phase inversion with respect to a state $|x\rangle$ changes the phase of this particular state by an amount of π and leaves all other states unchanged. Thus the phase inversion I_s with respect to the initial state $|s\rangle$ is defined by

$$\begin{aligned} I_s|s\rangle &= -|s\rangle, \\ I_s|x\rangle &= |x\rangle \quad (x \neq s). \end{aligned} \tag{7}$$

For two qubits, for example, its matrix representation is given by

$$I_s = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{8}$$

The controlled phase inversion I_{x_0} with respect to the searched state $|x_0\rangle$ is defined in an analogous way. As state $|x_0\rangle$ is not known explicitly but only implicitly through the property $f(x_0) = 1$ this transformation has to be performed with the help of the quantum oracle. This task can be achieved by preparing the ancilla of the oracle of Eq.(2) in state $|a_0\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. As a consequence one obtains the required properties for the phase inversion I_{x_0}, namely

$$\begin{aligned} |x, f(x) \oplus a_0\rangle &\equiv |x, 0 \oplus a_0\rangle \\ &= 1/\sqrt{2}(|x,0\rangle - |x,1\rangle) = |x, a_0\rangle \ \text{ for } \ x \neq x_0, \\ |x, f(x) \oplus a_0\rangle &\equiv |x, 1 \oplus a_0\rangle \\ &= 1/\sqrt{2}(|x,1\rangle - |x,0\rangle) = -|x, a_0\rangle \ \text{ for } \ x = x_0. \end{aligned} \tag{9}$$

One should bear in mind that this controlled phase inversion can be performed with the help of the quantum oracle of Eq.(2) only without explicit knowledge of state $|x_0\rangle$.

Grover's algorithm starts by preparing all m qubits of the quantum computer in state $|s\rangle = |0...0\rangle$. An elementary rotation in the direction of the searched state $|x_0\rangle$ with the property $f(x_0) = 1$ is achieved by the gate sequence

$$Q = -I_s \cdot H^{(2^m)} \cdot I_{x_0} \cdot H^{(2^m)}. \tag{10}$$

In order to rotate the initial state $|s\rangle$ into state $|x_0\rangle$ one has to perform a sequence of n such rotations and a final Hadamard transformation at the end, i.e.

$$|f\rangle = HQ^n|s\rangle. \tag{11}$$

The effect of the elementary rotation Q is demonstrated in Fig.3 for the case of three qubits, i.e. $m = 3$. The first Hadamard transformation $H^{(2^3)}$ prepares an equally weighted state. The subsequent quantum gate I_{x_0} inverts the amplitude of the searched state $|x_0\rangle = |111\rangle$. Together with the subsequent Hadamard transformation and the phase inversion I_s this gate sequence Q amplifies the probability amplitude of the searched state $|111\rangle$. In this particular case an additional Hadamard transformation finally prepares the quantum computer in the searched state $|111\rangle$ with a probability of 0.88.

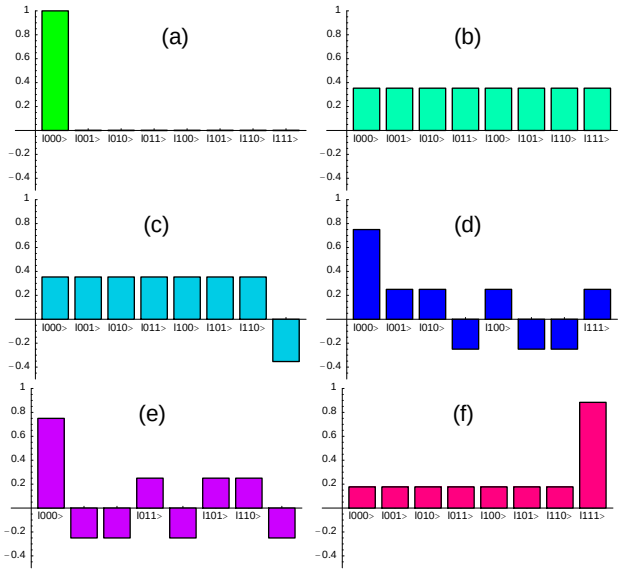


FIG. 3. Amplitude distributions resulting from the various quantum gates involved in Grover's quantum search algorithm for the case of three qubits: The quantum states which are prepared by these gates are (a) $|s\rangle = |000\rangle$, (b) $H^{(2^m)}|s\rangle$, (c) $I_{x_0}H^{(2^m)}|s\rangle$, (d) $H^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$, (e) $-I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$, (f) $-H^{(2^m)}I_sH^{(2^m)}I_{x_0}H^{(2^m)}|s\rangle$. The searched state $|x_0\rangle$ entering the Boolean function of Eq.(1) is assumed to be state $|111\rangle$.

In order to determine the dependence of the ideal number of repetitions n on the number of qubits m it is convenient to analyze the repeated application of the gate sequence Q according to Eq.(11) in terms of the two states $|s\rangle$ and $|v\rangle = H^{(2^m)}|x_0\rangle$ whose overlap is given by $\epsilon = \langle s|v\rangle = \langle s|H^{(2^m)}|x_0\rangle = 2^{-m/2}$ for m qubits. It is straightforward to show that the unitary gate sequence Q preserves the subspace spanned by these two states [3], i.e.

$$Q\begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix} = \begin{pmatrix} 1-4\epsilon^2 & 2\epsilon \\ -2\epsilon & 1 \end{pmatrix}\begin{pmatrix} |s\rangle \\ |v\rangle \end{pmatrix}. \qquad (12)$$

Thus Q acts like a rotation in the plane spanned by states $|s\rangle$ and $|v\rangle$. The angle of rotation is given by $\varphi = \arcsin(2\epsilon\sqrt{1-\epsilon^2})$.

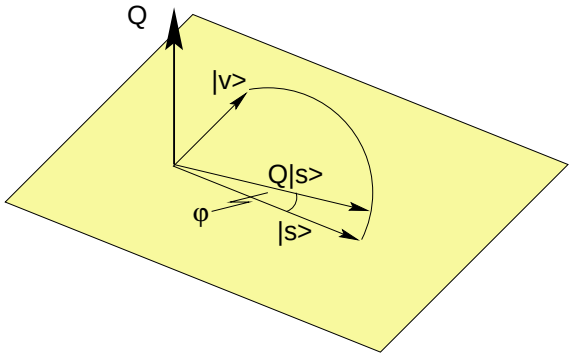


FIG. 4. Q is a rotation in the subspace spanned by states $|s\rangle$ and $|v\rangle$.

After j iterations the amplitude of state $|v\rangle$ is given by [7]

$$\sin\left[(2j+1)\epsilon\right]. \qquad (13)$$

Therefore, the optimal number n of repetitions of the gate sequence Q is approximately given by

$$n = \frac{\pi}{4\ \arcsin\left(2^{-m/2}\right)} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{2^m}\ \ (2^m \gg 1). \qquad (14)$$

B. Hamiltonian representation of Grover's algorithm

If the database contains many elements, i.e. $N \equiv \epsilon^{-2} \gg 1$, the repeated application of the elementary rotation which is essential for Grover's search algorithm can be described by a Hamiltonian quantum dynamics. The elementary rotation Q can be approximated by the relation

$$Q = \mathbf{1} - \tau\ i/\hbar \mathbf{H}_G(\epsilon) + O(\epsilon^2) \qquad (15)$$

which involves the Hamiltonian

$$\mathbf{H}_G = 2i\epsilon\frac{\hbar}{\tau}\ \left(|v\rangle\langle s| - |s\rangle\langle v|\right). \qquad (16)$$

The elementary time τ might be interpreted as the physical time required for performing the elementary rotation Q. The Hamiltonian of Eq.(16) describes the dynamics of a quantum mechanical two level system whose degenerate energy levels $|s\rangle$ and $|v\rangle$ are coupled by a time-independent perturbation. In lowest order of ϵ these degenerate energy levels are orthogonal. The resulting oscillations between these coupled energy levels are characterized by the Rabi frequency $\Omega = 2\langle s|v\rangle/\tau$. Correspondingly, the repeated application of the elementary rotation Q can be determined with the help of Trotter's product formula [17], namely

$$Q^n = (-I_s \cdot H^{(2^m)} \cdot I_{x_0} \cdot H^{(2^m)})^n = \exp\left(-\frac{i}{\hbar}\mathbf{H}_G\ \cdot \tau n\right) + O(\epsilon^2 n). \qquad (17)$$

Thus, in the framework of this Hamiltonian description applying the elementary rotation Q n times is equivalent to a time evolution of the effective two-level quantum system over a time interval of magnitude $n\tau$. This Hamiltonian description demonstrates that the physics behind Grover's quantum search algorithm is the same as the physics governing the Rabi oscillations between degenerate or resonantly coupled energy eigenstates. As the errors entering Eq.(17) are of order $O(\epsilon^2 n)$ this Hamiltonian description is applicable only as long as $\epsilon^2 n \equiv n/2^m \ll 1$. Thus for a given size of the database it is valid only as long as the number of iterations is sufficiently small, i.e. $n \ll 2^m$. However, as Grover's search algorithm needs approximately $(\pi\sqrt{2^m}/4)$ steps to find the searched item the main condition which restricts the validity of this Hamiltonian description is a large size of the database, i.e. $\epsilon^2 \equiv 1/N \ll 1$.

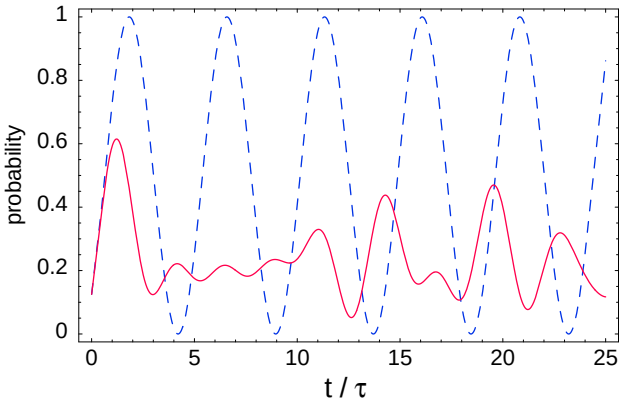


FIG. 5. The probability of being in state $|x_0\rangle$ after $n = t/\tau$ iterations of Grover's quantum search algorithm for three qubits: the ideal dynamics according to the Hamiltonian time evolution characterized by Eqs.(16) and (17) (dashed line); the non-ideal case of coherent errors as characterized by Eqs. (16), (17) and (18) (solid line) with detunings $\omega_1 = 0.5\ \langle s|v\rangle/\tau$, $\omega_2 = 0.3\ \langle s|v\rangle/\tau$, $\omega_3 = 0.2\ \langle s|v\rangle/\tau$.

C. An example of coherent errors

So far we have been concentrating on the ideal dynamics of Grover's quantum search algorithm. However, in practical applications it is very difficult to realize this search algorithm in an ideal way. Usually the ideal dynamics are affected by numerous perturbations. Physically one may distinguish two different kinds of errors, namely incoherent and coherent ones. Typically incoherent perturbations originate from a coupling of the physical qubits of a quantum computer to an uncontrollable environment. As a consequence the resulting errors are of a stochastic nature. Coherent errors may arise from non-ideal quantum gates which lead to a unitary but non-ideal time evolution of the quantum algorithm. A simple example of this latter type of errors are systematic detunings from resonance of the light pulses with which the required quantum gates are realized on the physical qubits. In the Hamiltonian formulation of Grover's algorithm such systematic detunings may be described by a perturbing Hamiltonian of the form

$$\mathbf{H}_d = \sum_{i=1}^{m} \hbar\omega_i \sigma_z^{(i)}. \tag{18}$$

In Eq.(18) it has been assumed that Grover's quantum algorithm is realized by m qubits and that the i-th qubit is detuned with respect to the ideal transition frequency by an amount ω_i. The Pauli spin-operator of the i-th qubit is denoted $\sigma_z^{(i)}$. In the presence of these systematic detunings and for a large number of qubits the dynamics of Grover's algorithm are described by the Hamiltonians of Eqs.(16) and (18).

In order to obtain insight into the influence of this type of coherent errors the performance of Grover's algorithm under repeated applications of the elementary rotation Q is depicted in Fig. 5. The dynamics of the ideal Grover algorithm are depicted by the dashed line for the case of three qubits, i.e. $m = 3$. The Rabi oscillations with frequency $\Omega = 2\langle v|s\rangle/\tau$ are clearly visible. The solid line shows the probability of observing the quantum computer in state $|x_0\rangle$ in a case in which all the qubits are detuned from their ideal resonance frequency. One notices the deviations from the ideal behaviour. Due to the coherent nature of the errors the time evolution of the non-ideal algorithm exhibits revival phenomena [18].

III. ERROR AVOIDING QUANTUM CODES

In general there are two different strategies for correcting errors in quantum information processing. If nothing is known about the physical origin of the errors affecting a qubit one can use *general quantum error correcting schemes*. They may be viewed as generalizations of classical error correction techniques to the quantum domain [10–12]. Typically they involve a suitably chosen quantum code and a sequence of quantum measurements. This code has to map all possible states which may result from arbitrary environmental influences onto orthogonal states. According to basic postulates of quantum theory these orthogonal quantum states can be distinguished and based on the result of a control measurement one may restore the original quantum state. So far these general techniques have been applied mainly to the stabilization of static quantum memories [19]. It is still an open question whether these general methods are also useful and efficient for the dynamical stabilization of quantum algorithms.

The second possible error correction strategy which seems to be well adopted also for stabilizing quantum algorithms is based on *error avoiding quantum codes* [13,14]. However, these latter methods are applicable only, if the physical origin of the errors is known. The

main idea is to encode the quantum information in those subspaces of the Hilbert space which are not affected by the errors. This aim is achieved by restricting oneself to degenerate eigenspaces of the relevant error operators. Thus, in the special case of a single error operator, say $\mathbf{E}$, the basis states $\{|\psi_i\rangle\}$ of such an error free subspace have to fulfill the relation

$$\mathbf{E}|\psi_i\rangle = c\,|\psi_i\rangle. \tag{19}$$

In the above mentioned example of coherent errors which may affect Grover's algorithm this error operator is given by the Hamiltonian of Eq.(18), i.e. $\mathbf{E} = \mathbf{H}_d$. It is crucial for the success of an error avoiding code that the eigenvalue c of Eq.(19) does not depend on the states belonging to the error free subspace. This implies that all possible elements of the error free subspace of the general form $\sum_i \alpha_i|\psi_i\rangle$ are affected by the error operator in the same way, i.e.

$$\mathbf{E}(\sum_i \alpha_i|\psi_i\rangle) = c(\sum_i \alpha_i|\psi_i\rangle). \tag{20}$$

It is apparent that a non-trivial error avoiding code is possible only, if the eigenspace of the error operator $\mathbf{E}$ is degenerate.

A. An error avoiding quantum code stabilizing coherent errors

As an example for an error avoiding quantum code let us consider the case of coherent errors which may affect Grover's quantum algorithm and which can be characterized by the Hamiltonian $\mathbf{H}_d$ of Eq.(18). In the simple case of equal detunings, i.e. $\omega_1 = ... = \omega_m \equiv \omega$, the error operator $\mathbf{E}$ reduces to the form

$$\mathbf{H}_e = \hbar\omega \sum_{i=1}^{m} \sigma_z^{(i)}. \tag{21}$$

It is easy to find highly degenerate error free subspaces of this error operator. All states with a fixed number of ones and zeroes constitute a degenerate eigenspace of $\mathbf{H}_e$. For an even number of qubits it is possible to find an error avoiding subspace with eigenvalue $c = 0$ so that

$$(\mathbf{H}_G + \mathbf{H}_e)\,|\psi\rangle = \mathbf{H}_G|\psi\rangle \tag{22}$$

for all elements $|\psi\rangle$ of this subspace. For this purpose one is looking for quantum states with zero total spin. For four qubits, for example, this subspace is defined by the basis vectors $|0011\rangle, |0101\rangle, |0110\rangle, |1001\rangle, |1010\rangle, |1100\rangle$ and involves all states with the same number of zeros and ones. Four of these states may be used as a basis for the state space of two *logical* qubits. For these eigenstates the error Hamiltonian $\mathbf{H}_e$ maps onto zero, e.g.

$$\mathbf{H}_e|0011\rangle = \hbar\omega \sum_{i=1}^{m=4} \sigma_z^{(i)}|0011\rangle = \hbar\omega(1+1-1-1)|0011\rangle = 0.$$

This particular error avoiding code works ideal for equal detunings of all qubits from resonance. It is formed by quantum states which factorize in the computational basis. So it is expected that in this error free subspace the encoding of quantum information and the implementation of quantum gates is considerably easier than in cases in which the error avoiding codes involve entangled quantum states.

B. Implementation of quantum gates in an error free subspace

To realize a quantum algorithm in an error free subspace one has to implement the necessary quantum gates in such a way that they do not mix the error free subspace with its orthogonal complement [20]. Consider two logical qubits, for example, which are encoded by four physical qubits. For this purpose one may choose the states $|0011\rangle, |0101\rangle, |0110\rangle, |1001\rangle$ which have been mentioned in the previous subsection. This error avoiding code works ideal for stabilizing Grover's algorithm with respect to the error operator $\mathbf{H}_e$ of Eq.(21) provided it is possible to realize the required unitary transformations, namely Hadamard transformations and the controlled phase inversions.

Consider as an example a Hadamard transformation which acts in a two dimensional error avoiding subspace of this kind. Thus it is assumed that the two basis states of this error avoiding code are given by $|01\rangle$ and $|10\rangle$ and that they involve two physical qubits. Thus, we are looking for a transformation which performs the mappings

$$\begin{aligned} |01\rangle &\rightarrow 1/\sqrt{2}(|01\rangle + |10\rangle), \\ |10\rangle &\rightarrow 1/\sqrt{2}(|01\rangle - |10\rangle) \end{aligned} \tag{23}$$

and which does not mix the subspace spanned by $|01\rangle$ and $|10\rangle$ with the orthogonal space spanned by the basis states $|00\rangle$ and $|11\rangle$. In matrix notation we are looking for a unitary matrix of the form

$$\begin{pmatrix} * & 0 & 0 & * \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ * & 0 & 0 & * \end{pmatrix} \tag{24}$$

with $*$ denoting arbitrary entries which ensure unitarity. Such a transformation can be achieved by the gate sequence $CNOT_{21}(\mathbf{1} \otimes \tilde{H}^{(2)})CNOT_{21}$ with $\tilde{H}^{(2)} = -i\sigma_y H^{(2)}$. Thereby $CNOT_{21}$ is a controlled-not operation with the first qubit as the target and the second qubit as the control qubit and σ_y is the Pauli Matrix. Thus in matrix notation this relation yields

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad (25)$$

Obviously the final result does not mix the error avoiding subspace with its orthogonal complement. But in the intermediate steps such a mixing takes place. However, for practical purposes it is enough to ensure that the time spent by the quantum computer in the orthogonal complement of the error avoiding subspace is sufficiently small so that the resulting errors can be neglected for all practical purposes. Under these circumstances it is expected that the implementation of quantum algorithms in error avoiding subspaces is a powerful tool for stabilizing quantum codes.

C. Code size of error avoiding quantum codes

In order to estimate the redundancy which has to be introduced for stabilizing a quantum algorithm by an error avoiding quantum code let us consider the particular example of Sec. IIIA in more detail. It has been argued that in the case of coherent errors which can be characterized by the Hamiltonian of Eq.(21) an error avoiding quantum code can be constructed from basis states with equal numbers of ones and zeroes. In order to minimize the redundancy it is desirable to maximize the dimension of the resulting error avoiding subspace. If one starts with m physical qubits the dimension $D(m,q)$ of the corresponding error avoiding subspace with q qubits in state $|1\rangle$ and $(m-q)$ qubits in state $|0\rangle$, for example, is given by

$$D(m,q) = \begin{pmatrix} m \\ q \end{pmatrix} \equiv \frac{m!}{q!(m-q)!}. \quad (26)$$

From elementary properties of binomial coefficients it is clear that $D(m,q)$ is maximum for $q = m/2$. Thus for an even number of qubits m the largest possible dimension of the resulting error avoiding subspace is given by

$$D(m,m/2) = \frac{m!}{[(m/2)!]^2} \rightarrow 2^m \sqrt{\frac{2}{m\pi}} \quad (m \gg 1). \quad (27)$$

Thus, in this case it is possible to encode

$$l = \log_2 D(m,m/2) \rightarrow m - \frac{\log_2 m}{2} + \log_2 \sqrt{2/\pi} \quad (m \gg 1) \quad (28)$$

logical qubits with m physical ones. It is instructive to compare the redundancy of this error avoiding code as described by Eq.(28) with the ones resulting from general error correcting quantum codes which saturate the quantum Hamming bound [15,21]. If one wants to correct arbitrary errors of maximum length t with a general error correcting quantum code the number of physical and logical qubits m and l have to fulfill the so called quantum Hamming bound [10,15,21], i.e.

$$2^l \sum_{r=0}^{t} 3^r \begin{pmatrix} m \\ r \end{pmatrix} \leq 2^m. \quad (29)$$

This inequality reflects the fact that in a general error correcting quantum code the action of different error operators onto any of the logical qubits must lead to orthogonal quantum states. The dimension of the resulting Hilbert space as described by the left hand side of the inequality (29) has to be smaller than the dimension of the Hilbert space of all physical qubits. Thus the number of logical qubits obtainable by a general error correcting code which is capable of correcting all possible errors of maximum length one, i.e. $t = 1$, cannot be larger than

$$l_> = m - \log_2(3m+1). \quad (30)$$

Comparing Eq.(28) with Eq.(30) one realizes that the redundancy of this particular error avoiding quantum code is smaller than the one resulting from saturating the Hamming bound with a general error correcting code capable of correcting errors of maximum length one, i.e.

$$l - l_> \rightarrow \frac{1}{2}\log_2 m + \log_2 \frac{3\sqrt{2}}{\sqrt{\pi}} > 0 \quad (m \gg 1). \quad (31)$$

However, this reduction of redundancy is based on the fact that the error avoiding code obeying Eq.(28) can stabilize errors only which are described by the Hamiltonian of Eq.(21). Usually more general errors cannot be corrected with this code.

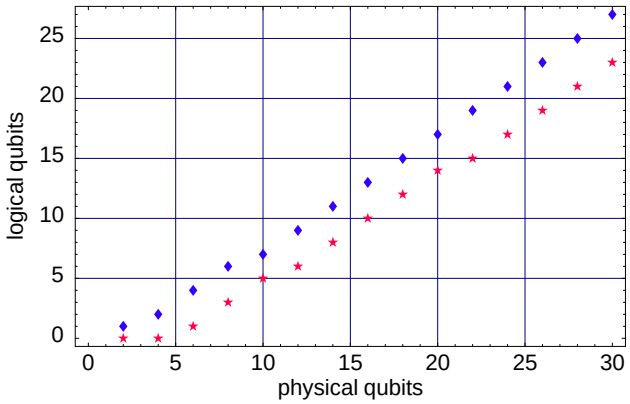


FIG. 6. Maximum number of logical qubits l versus number of physical qubits m for the error avoiding quantum codes which are capable of stabilizing the error operator of Eq.(21) (diamonds) (compare with Eq.(28)). The corresponding relation $l_>(m)$ of Eq.(30) characterizing the quantum Hamming bound is indicated by stars.

IV. NUMERICAL EXAMPLES

In the previous section we have developed an error avoiding quantum code which is capable of correcting coherent errors. These errors were assumed to be caused by

systematic detunings of the physical qubits of the quantum computer from the frequency of the laser pulses implementing the action of the quantum gates. This error avoiding quantum code works perfect provided all physical qubits are detuned from the frequency of these laser pulses by the same amount. However, in realistic situations this case is scarcely realized. For the realistic assumption of unequal detunings in general the eigenstates of $\mathbf{H}_d$ are non-degenerate so that it is not possible to construct a perfect error avoiding quantum code. Therefore the practical question arises whether the presented error avoiding quantum code of Sec. III is still useful for stabilizing quantum algorithms against arbitrary systematic detunings.

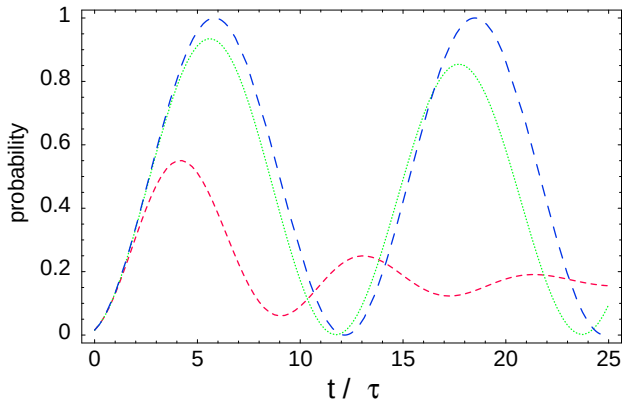


FIG. 7. Probability of finding the quantum computer in the searched state $|x_0\rangle$ after $n = t/\tau$ iterations: ideal dynamics without detunings for 6 qubits(dashed line), with detunings and without error avoiding encoding for 8 qubits(dotted line), with detunings and with error avoiding encoding using 8 physical qubits which can encode the quantum information of 6 logical qubits (solid line). For the latter two cases the magnitude of the detunings ω_i of the 8 qubits which determine the error operator of Eq.(18) are given by $\omega_i\tau/\langle v|s\rangle = 0.92065$, 1.1436, 0.71449, 1.39566, 1.29707, 0.70149, 1.19195, 1.00343.

The dynamics of Grover's algorithm in the presence of arbitrary detunings are depicted in Fig. 7. The dashed line represents the ideal dynamics in the absence of detunings for the case of 6 qubits as evaluated from the Hamiltonian of Eq.(16). The characteristic Rabi oscillations are clearly apparent. The corresponding dynamics for 8 qubits in the presence of arbitrarily chosen detunings are depicted by the dotted line in Fig.7. It is apparent that in this case a quantum search for state $|x_0\rangle$ is not successful at all. However, as apparent from the solid line of Fig. 7 encoding the quantum information by the error avoiding code of Sec.III improves the performance considerably. Despite the fact that this error avoiding code has not been designed for these detunings it almost succeeds in finding the searched quantum state $|x_0\rangle$ after a number of iterations which is close to the ideal case (compare with Eq.(14)).

In order to obtain more insight into the stabilizing properties of this error avoiding code let us investigate the probability of success in the presence of arbitrary detunings in more detail. For this purpose we consider 8 physical qubits whose detunings ω_i are distributed randomly according to a normal distribution. According to Fig.6 these 8 physical qubits are capable of encoding 6 logical qubits. In Fig. 8 the average value of the maximum probability of finding the quantum computer in the searched state $|x_0\rangle$ is depicted for various values of the variance of the randomly chosen detunings. The lower sequence of dots (stars) refers to Grover's algorithms without error avoiding encoding and the upper sequence of points (diamonds) refers to error avoiding encoding according to Sec. III. It is apparent that error avoiding encoding is very successful as long as the differences between the detunings of the qubits is sufficiently small. Only in extreme cases in which these differences become comparable to the typical magnitudes of the detunings this type this error avoiding code is no longer capable of stabilizing Grover's algorithm in a satisfactory way.

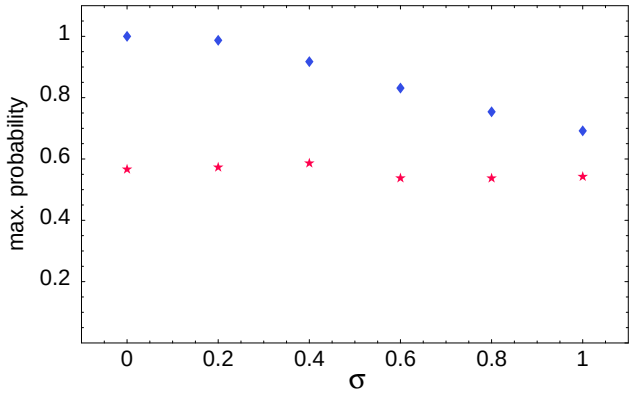


FIG. 8. Average maximum probability of success for Grover's algorithm with 8 qubits in the presence of randomly chosen detunings: with error avoiding encoding according to Sec. III (diamonds); without error avoiding encoding (stars). The detunings ω_i of the 8 physical qubits were chosen randomly according to a normal distribution with mean value $\overline{\omega} = 0.5\langle v|s\rangle/\tau$. The corresponding variance σ of these detunings is plotted on the x-axis in units of the mean value $\overline{\omega}$.

V. SUMMARY AND CONCLUSIONS

It has been demonstrated that error avoiding quantum codes may offer efficient methods for stabilizing quantum codes dynamically against those types of errors whose physical origin is known. As a particular example we discussed the stabilization of Grover's quantum search algorithm against coherent errors which may arise from systematic detunings of the physical qubits from the frequency of the light pulses implementing the quantum gates. Though originally the error avoiding quantum

code has been constructed for the special case of equal detunings of all the qubits it has been shown that it is also capable of stabilizing this quantum algorithm in other cases to a satisfactory degree. The proposed error avoiding quantum code consists of quantum states only which are factorizable in the computational basis. This may offer advantages as far as the implementation of the necessary quantum gates in this error free subspace is concerned. Furthermore, this quantum code has also other noteworthy properties, such as a redundancy which is lower than the one of an optimal error correcting quantum code saturating the quantum Hamming bound. Though the stabilizing ability of error avoiding quantum codes has been demonstrated for one particular quantum code and one particular class of coherent errors only it is expected that similar capabilities are also found in more general cases which may also involve incoherent errors.

This work is supported by the DFG within the SPP 'Quanteninformationsverarbeitung'. Stimulating discussions with Thomas Beth, Markus Grassl and Dominik Janzing are acknowledged.

[1] R.P. Feynman, Int. J. Theor. Phys. **21** 467-488, 1982.
[2] W.Shor, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, edited by S.Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p 124.
[3] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997); **80**, 4329 (1998).
[4] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[5] N. Gershenfeld and I. Chuang, Science **275**, 350 (1997).
[6] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **75**, 3788 (1995).
[7] M. Boyer, G. Brassard, P. Hoyer, A. Tapp, Fortschr. Phys. **46**, 493 (1998).
[8] I.L. Chuang, N. Gershenfeld and M.Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
[9] C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **78**, 3971 (1997).
[10] R. Laflamme, C. Miquel, J.P. Paz and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[11] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[12] A. Steane, Rep.Prog.Phys. **61**, 117-173 (1998).
[13] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[14] P. Zanardi, Phys. Rev. A. **57**, 3276 (1998); **60**, R729 (1999).
[15] D. Welsh, *Codes and Cryptography*, (Clarendon Press, Oxford,1988).
[16] C. Zalka, Phys. Rev. A **60**, 2746 (1999).
[17] L. Schulman, *Techniques and Applications of Path Integration* (Wiley, New York, 1981).
[18] I. Sh. Averbukh and N. F. Perelman, Phys. Lett. A **139**, 449 (1989).
[19] T. Pellizzari, Th. Beth, M. Grassl, and J. Müller-Quade, Phys. Rev. A. **54**, 2698 (1996).
[20] D. Bacon, J.Kempe, D.A. Lidar and K.B. Whaley, lanl e-print quant-ph/9909058.
[21] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).